UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,725	02/06/2002	Kaoru Murase	2002_0184A	4067

513 7590 02/01/2008

WENDEROTH, LIND & PONACK, L.L.P.
2033 K STREET N. W.
SUITE 800
WASHINGTON, DC 20006-1021

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	**PAPER NUMBER**
2131	

MAIL DATE	DELIVERY MODE
02/01/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/066,725	MURASE ET AL.	
	Examiner	Art Unit	
	Matthew T. Henning	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 October 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,2,4,7-14,17,18,22-26,28-31,34-36,38-41,44 and 46-48* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,2,4,7-14,17,18,22-26,28-31,34-36,38-41,44 and 46-48* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *06 February 2002* is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

This action is in response to the communication filed on 10/29/2007.

DETAILED ACTION

Response to Arguments

Applicant's arguments with respect to the prior art rejections of claims 1-2, 4, 7-14, 17-18, 22-26, 28-31, 34-36, 38-41, 44, and 46-48 have been considered but are moot in view of the new ground(s) of rejection.

Claims 1-2, 4, 7-14, 17-18, 22-26, 28-31, 34-36, 38-41, 44, and 46-48 have been examined, while claims 3, 5-6, 15-16, 19-21, 27, 32-33, 37, 42-43, and 45 have been cancelled.

All objections and rejections not set forth below have been withdrawn.

Specification

The specification is objected to as failing to provide proper antecedent basis for the claimed subject matter. See 37 CFR 1.75(d)(1) and MPEP § 608.01(o). Correction of the following is required:

Claim 1 recites a computing device comprising "a processor". The examiner is unable to find support for this limitation, and the applicants have not shown where support can be found in the specification. The examiner notes that there is support for "a microcomputer".

Newly added claims 46-48 recite destroying a first sector of all of the I pictures **regardless of the processing capacity of the data nullification device**". The examiner is unable to find support for this limitation, and the applicants have not shown where support can be found in the specification.

See the rejection of claims 19-21 under 35 USC 112 1st Paragraph below.

Claim Rejections - 35 USC § 112

The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-2, 4, 7-14, 17-18, 22-24, and 46-48 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

Claim 1 recites a computing device comprising "a processor". The examiner is unable to find support for this limitation, and the applicants have not shown where support can be found in the specification. The examiner notes that there is support for "a microcomputer".

Newly added claims 46-48 recite destroying a first sector of all of the I pictures **regardless of the processing capacity of the data nullification device**". The examiner is unable to find support for this limitation, and the applicants have not shown where support can be found in the specification.

Therefore, claims 1-2, 4, 7-14, 17-18, 22-24, and 46-48 are rejected for failing to meet the written description requirement of 35 USC 112 1st Paragraph.

Claim Rejections - 35 USC § 103

Claims 1-2, 4, 7-8, 12-14, 22-26, 28, 31, 34-36, 38, 41, and 44, are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsushita (US Patent Number 6,694,002) hereinafter

referred to as Matsushita, and further in view of Masinter (US Patent Number 5,742,807), and further in view of Prasad (US Patent Number 5,826,083).

The applied references have a common assignee with the instant application. Based upon the earlier effective U.S. filing date of the reference, it constitutes prior art only under 35 U.S.C. 102(e). This rejection under 35 U.S.C. 103(a) might be overcome by: (1) a showing under 37 CFR 1.132 that any invention disclosed but not claimed in the reference was derived from the inventor of this application and is thus not an invention "by another"; (2) a showing of a date of invention for the claimed subject matter of the application which corresponds to subject matter disclosed but not claimed in the reference, prior to the effective U.S. filing date of the reference under 37 CFR 1.131; or (3) an oath or declaration under 37 CFR 1.130 stating that the application and reference are currently owned by the same party and that the inventor named in the application is the prior inventor under 35 U.S.C. 104, together with a terminal disclaimer in accordance with 37 CFR 1.321(c). This rejection might also be overcome by showing that the reference is disqualified under 35 U.S.C. 103(c) as prior art in a rejection under 35 U.S.C. 103(a). See MPEP § 706.02(l)(1) and § 706.02(l)(2).

Regarding claim 1, Matsushita disclosed a computing device comprising: a processor (See Matsushita Fig. 1 Element 11); and a data nullification device for nullifying at least a part of target data recorded on a recording medium, the target data being made up a plurality of data blocks (See Matsushita Abstract and Figs. 1 and 4), the data nullification device comprising: a first judging unit (See Matsushita Figs. 1 Element 18) operable to judge, for each data block of the target data, whether the data block needs be nullified (See Matsushita Fig. 4 Step S3a and Col. 6 Lines 31-57); and a nullifying unit (See Matsushita Fig. 1 Element 21) operable to, when a

predetermined number of data blocks are judged as needing to be nullified or when one or more data blocks whose total amount of data reaches a predetermined amount are judged as needing to be nullified, nullify the judged data blocks (See Matsushita Col. 6 Lines 41-54), but failed to specifically disclose a "sequential" nullifying unit operable to destroy only a part of a data block judged as needing to be nullified, the part including data necessary to utilize remaining parts of the data block; a processing capacity judging unit operable to judge whether the data nullification device has a processing capacity sufficient to destroy all data which is judged as needing to be nullified; and a total nullifying unit operable to destroy data which is included in the data block judged as needing to be nullified and is not destroyed by the sequential nullifying unit, when the processing capacity judging unit judges that the data nullification device has the sufficient processing capacity. However, Matsushita did disclose that the new data blocks were recorded to the same medium as the judged data blocks (See Matsushita Col. 5 Line 45 – Col. 6 Line 57 "hard disk"), and disclosed "zeroing" the previously judged data (See Matsushita Col. 6 Lines 51-54).

Conversely, Masinter teaches that for data which is encrypted by a key, it is much simpler to destroy the decryption key for the data, than to destroy all of the encrypted data itself (See Masinter Col. 2 Lines 57-61) and that the key used to encrypt and decrypt the data can be a hash of the data (See Masinter Col. 2 Lines 54-56).

Also, it was further well known that even without the knowledge of an encryption key, encrypted data can be recovered through a very long process known as a brute force attack.

Prasad teaches a system which self-regulates its consumption of CPU cycles involving monitoring the CPU load (See Prasad Abstract). Prasad further teaches that a CPU intensive

application includes mainline logic that are designed to be able to be executed at different functional levels, consuming different rates of CPU cycles, and self-regulating logic for monitoring CPU load, and decrementally adapting the CPU intensive application to decreasingly lower functional levels, and therefore lower rates of CPU cycle consumptions, in accordance to a set of adaptive policies. The set of adaptive policies specify a number of domain specific responses to various CPU load conditions. (See Prasad Col. 1 Lines 48-59) Prasad teaches that when the CPU load surpasses a threshold, the application is decreased to a lower functional level and vice versa. (See Prasad Summary of the invention and Col. 3 Lines 7-46).

It would have been obvious to employ the teachings of Masinter and Prasad in the content erasing system of Matsushita by employing a function which monitors the load on the processor of Matsushita, and when the load is above a certain threshold overwriting only the decryption key for each packet judged to be erased, and when the load is below the threshold overwriting each packet judged to be erased. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the system to adapt to processing load conditions, by destroying the packets using different methods which vary in CPU intensity during varying conditions of CPU load, while still ensuring that erased packets are not accessible via brute force attack.

Regarding claim 25, Matsushita disclosed A data nullification program embodied on a computer readable medium for nullifying at least a part of target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification program causing a computer to execute of a method comprising: judging, for each data block of the target data, whether the data block needs to be nullified (See Matsushita Fig. 4 Step S3a and

Col. 6 Lines 31-57); receiving continuously transmitted data from an external device, and setting the received data as a new data block (See Matsushita Col. 5 Line 45 – Col. 6 Line 12); and overwriting, when predetermined number of data blocks are judged as needing to be nullified or when one or more data blocks whose total amount of data reaches a predetermined amount are judged as needing to be nullified, the judged data blocks (See Matsushita Col. 6 Lines 41-54) but failed to specifically disclose a "sequential" nullifying unit operable to destroy only a part of a data block judged as needing to be nullified, the part including data necessary to utilize remaining parts of the data block; a processing capacity judging unit operable to judge whether the data nullification device has a processing capacity sufficient to destroy all data which is judged as needing to be nullified; and a total nullifying unit operable to destroy data which is included in the data block judged as needing to be nullified and is not destroyed by the sequential nullifying unit, when the processing capacity judging unit judges that the data nullification device has the sufficient processing capacity. However, Matsushita did disclose that the new data blocks were recorded to the same medium as the judged data blocks (See Matsushita Col. 5 Line 45 – Col. 6 Line 57 "hard disk"), and disclosed "zeroing" the previously judged data (See Matsushita Col. 6 Lines 51-54).

Conversely, Masinter teaches that for data which is encrypted by a key, it is much simpler to destroy the decryption key for the data, than to destroy all of the encrypted data itself (See Masinter Col. 2 Lines 57-61) and that the key used to encrypt and decrypt the data can be a hash of the data (See Masinter Col. 2 Lines 54-56).

Also, it was further well known that even without the knowledge of an encryption key, encrypted data can be recovered through a very long process known as a brute force attack.

Prasad teaches a system which self-regulates its consumption of CPU cycles involving monitoring the CPU load (See Prasad Abstract). Prasad further teaches that a CPU intensive application includes mainline logic that are designed to be able to be executed at different functional levels, consuming different rates of CPU cycles, and self-regulating logic for monitoring CPU load, and decrementally adapting the CPU intensive application to decreasingly lower functional levels, and therefore lower rates of CPU cycle consumptions, in accordance to a set of adaptive policies. The set of adaptive policies specify a number of domain specific responses to various CPU load conditions. (See Prasad Col. 1 Lines 48-59) Prasad teaches that when the CPU load surpasses a threshold, the application is decreased to a lower functional level and vice versa. (See Prasad Summary of the invention and Col. 3 Lines 7-46).

It would have been obvious to employ the teachings of Masinter and Prasad in the content erasing system of Matsushita by employing a function which monitors the load on the processor of Matsushita, and when the load is above a certain threshold overwriting only the decryption key for each packet judged to be erased, and when the load is below the threshold overwriting each packet judged to be erased. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the system to adapt to processing load conditions, by destroying the packets using different methods which vary in CPU intensity during varying conditions of CPU load, while still ensuring that erased packets are not accessible via brute force attack.

Matsushita further failed to disclose the method being implemented in software. However, it was well know that the functionality of a system can be implemented in software in order to provide for greater ease of upgrade. Therefore, it would have been obvious to the

ordinary person skilled in the art at the time of invention to implement the system of Matsushita in software running on a processor. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to ensure the system could be easily upgraded.

Regarding claim 35, Matsushita disclosed a data nullification method for nullifying at least a part of target data recorded on a recording medium, the target data being made up of a plurality of data blocks, the data nullification method comprising: judging, for each data block of the target data, whether the data block needs to be nullified (See Matsushita Fig. 4 Step S3a and Col. 6 Lines 31-57); receiving continuously transmitted data from an external device, and setting the received data as a new data block (See Matsushita Col. 5 Line 45 – Col. 6 Line 12); and overwriting, when predetermined number of data blocks are judged as needing to be nullified or when one or more data blocks whose total amount of data reaches a predetermined amount are judged as needing to be nullified, the judged data blocks (See Matsushita Col. 6 Lines 41-54) but failed to specifically disclose a "sequential" nullifying unit operable to destroy only a part of a data block judged as needing to be nullified, the part including data necessary to utilize remaining parts of the data block; a processing capacity judging unit operable to judge whether the data nullification device has a processing capacity sufficient to destroy all data which is judged as needing to be nullified; and a total nullifying unit operable to destroy data which is included in the data block judged as needing to be nullified and is not destroyed by the sequential nullifying unit, when the processing capacity judging unit judges that the data nullification device has the sufficient processing capacity. However, Matsushita did disclose that the new data blocks were recorded to the same medium as the judged data blocks (See Matsushita Col. 5

Line 45 – Col. 6 Line 57 "hard disk"), and disclosed "zeroing" the previously judged data (See Matsushita Col. 6 Lines 51-54).

Conversely, Masinter teaches that for data which is encrypted by a key, it is much simpler to destroy the decryption key for the data, than to destroy all of the encrypted data itself (See Masinter Col. 2 Lines 57-61) and that the key used to encrypt and decrypt the data can be a hash of the data (See Masinter Col. 2 Lines 54-56).

Also, it was further well known that even without the knowledge of an encryption key, encrypted data can be recovered through a very long process known as a brute force attack.

Prasad teaches a system which self-regulates its consumption of CPU cycles involving monitoring the CPU load (See Prasad Abstract). Prasad further teaches that a CPU intensive application includes mainline logic that are designed to be able to be executed at different functional levels, consuming different rates of CPU cycles, and self-regulating logic for monitoring CPU load, and decrementally adapting the CPU intensive application to decreasingly lower functional levels, and therefore lower rates of CPU cycle consumptions, in accordance to a set of adaptive policies. The set of adaptive policies specify a number of domain specific responses to various CPU load conditions. (See Prasad Col. 1 Lines 48-59) Prasad teaches that when the CPU load surpasses a threshold, the application is decreased to a lower functional level and vice versa. (See Prasad Summary of the invention and Col. 3 Lines 7-46).

It would have been obvious to employ the teachings of Masinter and Prasad in the content erasing system of Matsushita by employing a function which monitors the load on the processor of Matsushita, and when the load is above a certain threshold overwriting only the decryption key for each packet judged to be erased, and when the load is below the threshold

overwriting each packet judged to be erased. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the system to adapt to processing load conditions, by destroying the packets using different methods which vary in CPU intensity during varying conditions of CPU load, while still ensuring that erased packets are not accessible via brute force attack.

Regarding claims 2, 26, and 36, Matsushita, Masinter, and Prasad disclosed that the recording medium stores sequence information that shows a sequence in which the plurality of data blocks were recorded onto the recording medium and the judging unit judges, in succession, the plurality of data blocks in the sequence shown by the sequence information, as needing to be nullified (See Matsushita Figs. 1 and 4, and Col. 6 Lines 29-57).

Regarding claim 4, Matsushita, Masinter, and Prasad disclosed that each data block has a length corresponding fixed transmission time period, a specified number of recording areas which are each used as a recording area of a data block are reserved on the recording medium (See Matsushita Col. 5 Line 66 – Col. 6 Line 6).

Regarding claims 7, 12, 28, 31, 38, and 41, Matsushita, Masinter, and Prasad disclosed a utilizing unit operable to utilize the target data recorded on the recording medium, wherein the judging unit data block which was utilized by in units of data blocks, further judges that each the utilizing unit needs nullified (See Matsushita Col. 6 Lines 29-57).

Regarding claim 8, and 13 Matsushita, Masinter, and Prasad disclosed that the target data is content data which is transmitted from an external device and recorded on the recording medium (See Matsushita Col. 5 Lines 45-65 and Abstract), the content data is accompanied with copy control information showing whether copying of the content data is permitted or prohibited

(See Matsushita Col. 5 Lines 51-53), the utilizing unit reproduces the content data recorded on the recording medium, in units of data blocks, and only if the copy control information accompanying the content data shows that the copying of the content data is prohibited, the judging unit judges that each data block which was reproduced by the utilizing unit needs to be nullified (See Matsushita Col. 6 Lines 31-54).

Regarding claim 14, Matsushita, Masinter, and Prasad disclosed that the target data is accompanied with copy control information showing whether copying of the target data permitted or prohibited (See Matsushita Col. 5 Lines 51-53), the utilizing unit records the on the recording medium, to another target data recorded recording medium, units of data blocks, and only if the copy control information accompanying the target data shows that the copying of the target data is prohibited, the judging unit judges that each data block on the recording medium which was recorded by the utilizing unit needs to be nullified (See Matsushita Col. 6 Lines 31-54 and Col. 6 Line 66 – Col. 7 Line 11).

Regarding claims 22, 34, and 44, Matsushita, Masinter, and Prasad disclosed that each data block recorded on the recording medium has been encrypted using an individual encryption key (See Matsushita Col. 5 Lines 57-62), and a decryption key for decrypting the encrypted data block is stored on the recording medium (See Matsushita Col. 5 Lines 57-62 and Col. 6 Lines 41-45), and the sequential nullifying unit destroying the decryption key when the data block is judged to be erased (See the rejection of claim 1 above).

Regarding claim 23, the combination of Matsushita, Masinter, and Prasad disclosed an acquiring unit operable to acquire the target data in an encoded form (See Matsushita Col. 6 Lines 41-45); a decoding unit operable to decode the encoded target data using a user key which

has been provided to authorized users in advance, to obtain the target data (See Matsushita Col. 6 Lines 41-45); a key generating unit operable to generate an arbitrary encryption key and a decryption key corresponding to the encryption key, for each data block of the target data (See Masinter Col. 5 Lines 40-48); a data encrypting unit operable to encrypt the data block using the encryption key so that the encrypted data block can be decrypted using the corresponding decryption key (See Masinter Col. 2 Lines 54-56); a key encrypting unit operable to encrypt the decryption key using an identifier unique to the data nullification device (See Masinter Col. 4 Paragraph 2); and recording unit operable to record the encrypted data block and the encrypted decryption key onto recording medium (See Matsushita Col. 5 Lines 45-65).

Regarding claim 24, the combination of Matsushita, Masinter, and Prasad disclosed that at least the decoding unit, the key generating unit, the data encrypting unit, and the key encrypting unit are contained in a single semiconductor chip (See Matsushita Fig. 1).

Claims 9-11, 29-30, and 39-40 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matsushita, Masinter, and Prasad as applied to claims 1, 25, and 35 above, and further in view of Garfinkle (US Patent Number 5,400,402).

Regarding claims 9, 29, and 39, Matsushita, Masinter, and Prasad disclosed judging whether data blocks needed to be nullified or not (See Matsushita Col. 51-54), but failed to disclose the data blocks having an expiration time at which they would need to be nullified.

Garfinkle teaches that downloaded content should be given a time limit and once the time limit is reached the content should be erased (See Garfinkle Col. 2 Lines 26-35).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Garfinkle in the content system Matsushita, Masinter, and

Prasad by providing a time limit with the content packets and erasing the content packets once the time limit was over. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to control the use of the received content.

Regarding claims 10, 30, and 40, see the rejection of claim 7 above.

Regarding claim 11, see the rejection of claim 8 above.

Claims 17, 18, and 46-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over the combination of Matsushita, Masinter, and Prasad as applied to claim 1 above, and further in view of Boyce et al. (US Patent Number 5,717,816) hereinafter referred to as Boyce.

Matsushita, Masinter, and Prasad disclosed nullification of MPEG data, which includes I pictures, B pictures, and P pictures (See the rejection of claim 1 above and Matsushita Col. 1), but failed to disclose a unit for destroying only an I picture or the first sector of an I picture.

Boyce teaches that an I frame is necessary to support trick play of an MPEG (See Boyce Col. 4 Lines 37-47).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Boyce in the content reproduction system of Matsushita, Masinter, and Prasad by providing a unit for destroying I-frames or parts thereof. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide a means for preventing trick play of an MPEG.

It further would have been obvious in this combination that in order delete the MPEG data entirely, the remaining portions of the I, B, and P, pictures would have been destroyed, and as discussed above, this would have been a more CPU intensive operation than destroying only a

portion of the I picture, and thus would be performed only when the CPU load was below a certain threshold as taught by Prasad. This would have been obvious because the ordinary person skilled in the art would have been motivated to allow the system to adapt to CPU loading conditions while still providing the desired functionality.

Conclusion

Claims 1-2, 4, 7-14, 17-18, 22-26, 28-31, 34-36, 38-41, 44, and 46-48 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Henning/
Assistant Examiner
Art Unit 2131

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100